REMARKS

Claims 1-7, 22-27 and 34 are pending and have been examined in the present application. Applicant wishes to thank the Examiner for acknowledging the election of the Restriction Requirement in paragraph 1 of the Office Action.

Claims 1, 6, 22, 26, and 34 have been amended to correct informalities as suggested by the Examiner in paragraph 4. No new matter has been added by the amendments.

In paragraph 6 of the Office Action, claims 22-27 are rejected under 35 U.S.C. 101, as being directed to non-statutory subject matter. Claim 22 has been amended to overcome the rejections made under 35 U.S.C. 101. Claim 22 has been amended to add steps that receive and output the input text denoted in the specification as a plain/cipher text. This plain/cipher text is tangible data that is transformed by the computer. The transformed plain/cipher text is output after the encryption/decryption. Since the claim receives and outputs a tangible result and not merely an idea or abstract concept, it places the claimed subject matter into a "safe harbor" and is allowable statutory subject matter.

In paragraph 8 of the Office Action, claims 1-2, 4, 7, 22, 24, 27, and 34 are rejected under 35 U.S.C. 102(a), as being anticipated by Page (Theoretical use of Cache Memory as a Cryptanalytic Side-Channel). The Examiner's rejection on this ground is respectfully traversed.

Independent claim 34 contains the limitation of generating transformation tables based on "whether the targeted transformation table exhibits a trend of increasing in the number of operation entries as a length of encryption time becomes longer." This limitation is neither disclosed nor suggested by Page. The Office Action cites section 4, 4.1, and 4.2 in Page in rejecting this limitation of claim 34. However, in the cited portions, Page only recites that the "S-box structures have been rearranged for easy array-style indexing" and that the equations in the pseudo-code implementation of DES "hold for a different sub-set of bits for each S-box in each transformation." This section does not teach or suggest how to identify a targeted transformation

table as explicitly recited in claim 34. Furthermore, the sections cited above recite a substitution transformation which are implemented by accesses to the S-box structures in memory but these section do not disclose the limitation where the transformation tables contain a predetermined number of entries where "the targeted transformation table is previously identified from the transformation tables depending on whether the targeted transformation table exhibits a trend of increasing in the number of operation entries as a length of encryption time becomes longer." As Page does not teach or suggest this feature of the invention of claim 34, withdrawal of the rejection of claim 34 on the basis of Page is therefore respectfully requested.

Claims 1 and 22 are stated in the Office Action to be directed to a hardware/software implementation of the method of claim 34 and are therefore allowable for at least the reasons stated above with regards to claim 34.

Claims 2, 4, and 7 depend from claim 1 and includes all of the limitations found therein. Claims 2, 4, and 7 include further limitations which, in combination with the limitations of claim 1 are neither disclosed nor suggested in the art of record. Therefore, claims 2, 4, and 7 are allowable.

Claims 24 and 27 depend from claim 22 and includes all of the limitations found therein. Claims 24 and 27 include further limitations which, in combination with the limitations of claim 22 are neither disclosed nor suggested in the art of record. Therefore, claims 24 and 27 are allowable.

In paragraph 10 of the Office Action, claims 3 and 23 are rejected under 35 U.S.C. 103(a), as being unpatentable over Page (Theoretical use of Cache Memory as a Cryptanalytic Side-Channel). Claims 3 and 23 depend from claims 1 and 22 respectively and are therefore allowable for at least the reasons stated above with regards to claims 1 and 22.

Further, Applicant requests clarification about the judicial notice taken in the Office Action of having the targeted transformation table loaded after the other transformation tables have been loaded into the cache memory. Cache memory, as known by the Applicant, is always a Random access memory (RAM) and there is no last-in-first-out (LIFO) scheme implemented in a RAM as

indicated in the Office Action. The benefit as mentioned in the Office Action for easy access to the targeted transformation table is not an issue with respect to a Cache memory as all of the memory in the cache is equally accessible. The Office Action's official notice therefore does not appear to be applicable to the present invention. Therefore, Applicant respectfully requests clarification of the judicial notice taken in the Office Action.

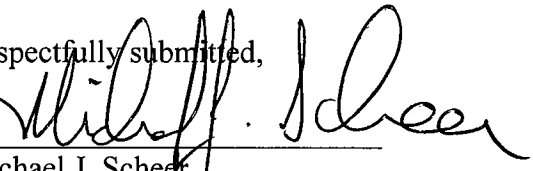
In paragraph 11 of the Office Action, dependant claims 5 and 25 are rejected under 35 U.S.C. 103(a), as being unpatentable over Page (Theoretical use of Cache Memory as a Cryptanalytic Side-Channel) in view of Lee (6,654,874). In paragraph 12 of the Office Action, dependant claims 6 and 26 are rejected under 35 U.S.C. 103(a), as being unpatentable over Page (Theoretical use of Cache Memory as a Cryptanalytic Side-Channel) in view of Ng et al. (6,725,329).

Claims 5 and 6 dependant from claim 1 and claim 25 and 26 depend from claim 22. Because the primary reference does not contain all the limitations recited in claims 1 and 22, the dependant claims are allowable because combining Lee and Ng et al. still does not cure the deficiencies. For at least this reason, claims 5, 6, 25, and 26 are allowable.

In view of the above amendment, applicant believes the pending application is in condition for allowance. No fee is believed to be due for this Amendment. Should any fees be required, please charge such fees to Deposit Account No. 50-2215.

Dated: September 28, 2007

Respectfully submitted,

By 

Michael J. Scheer
Registration No.: 34,425
DICKSTEIN SHAPIRO LLP
1177 Avenue of the Americas
New York, New York 10036-2714
(212) 277-6500
Attorney for Applicant